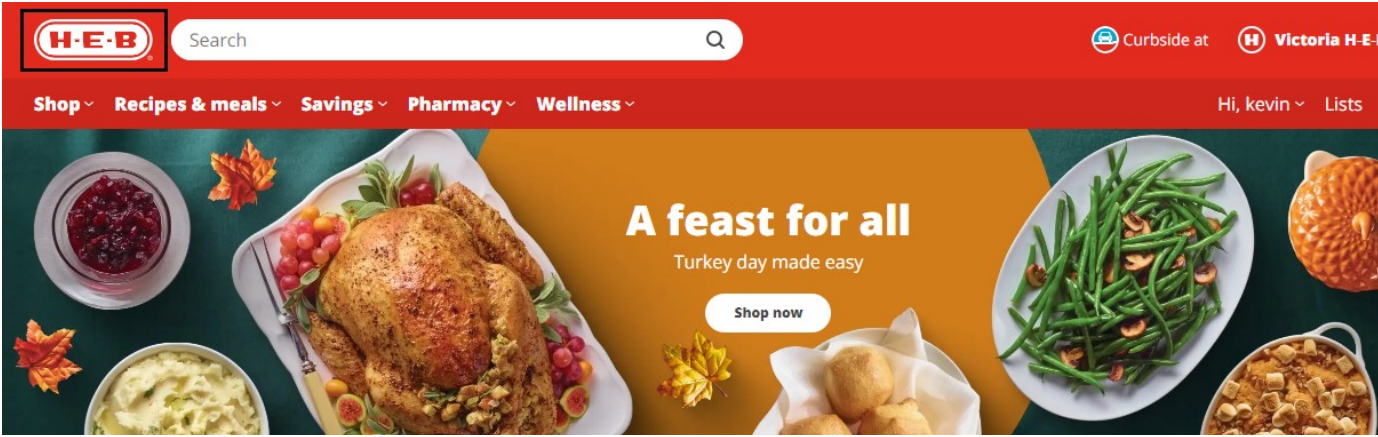
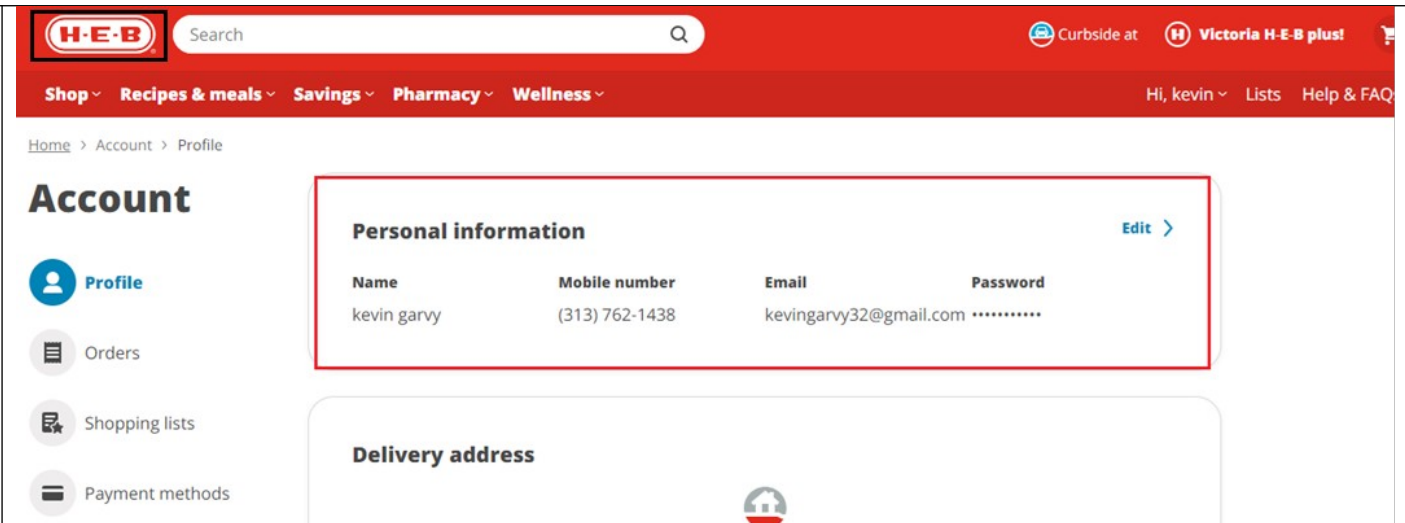
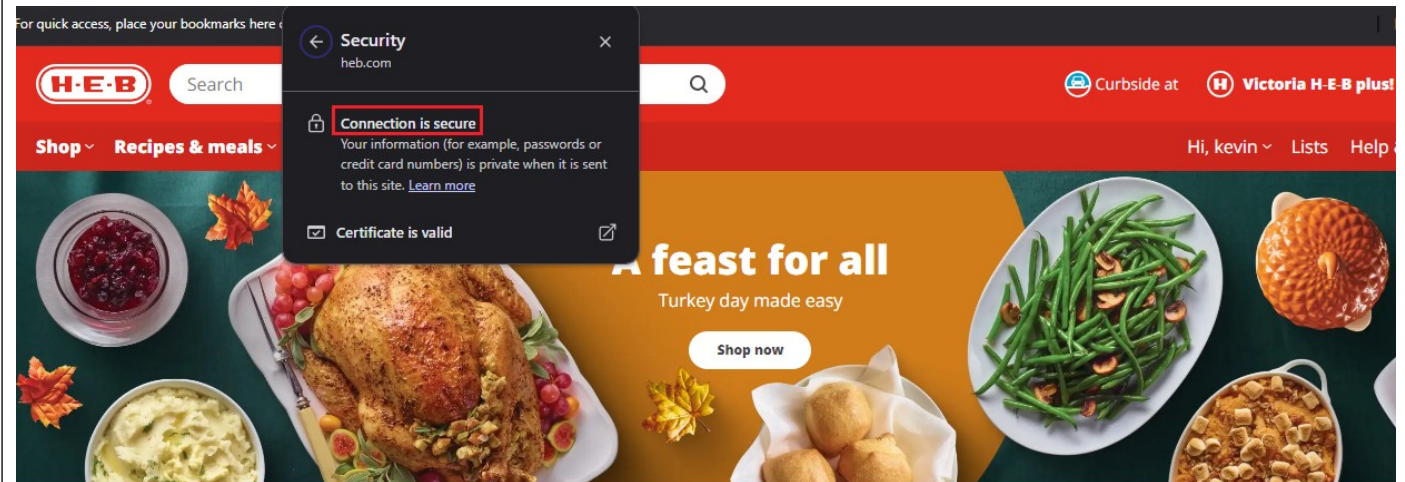


Exhibit 2







<p>US8677116B1</p> <p>1. A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:</p>	<p>H-E-B Grocery Company, LP's website "heb.com" ("The accused instrumentality")</p> <p>The accused instrumentality practices a method of using a computer system (e.g., authentication server of the accused instrumentality, etc.) to authenticate a user seeking to conduct at least one interaction (e.g., account login, food searches, etc.) with a secured capability provided by a computer (e.g., server of the accused instrumentality).</p> <p>As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, food searches, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access.</p>  <p>The screenshot shows the H-E-B website homepage. At the top is a red navigation bar with the H-E-B logo, a search bar, and links for 'Curbside at' and 'Victoria H-E-B'. Below the navigation bar are links for 'Shop', 'Recipes & meals', 'Savings', 'Pharmacy', and 'Wellness'. The main content area features a large image of a Thanksgiving meal with a roasted turkey, cranberry sauce, green beans, and mashed potatoes. The text 'A feast for all' and 'Turkey day made easy' is overlaid on the image, along with a 'Shop now' button. The URL 'https://www.heb.com/' is displayed at the bottom of the screenshot.</p> <p>https://www.heb.com/</p>
--	--



<https://www.heb.com/my-account/profile?showMobileView=Account%20Profile>



<https://www.heb.com/>

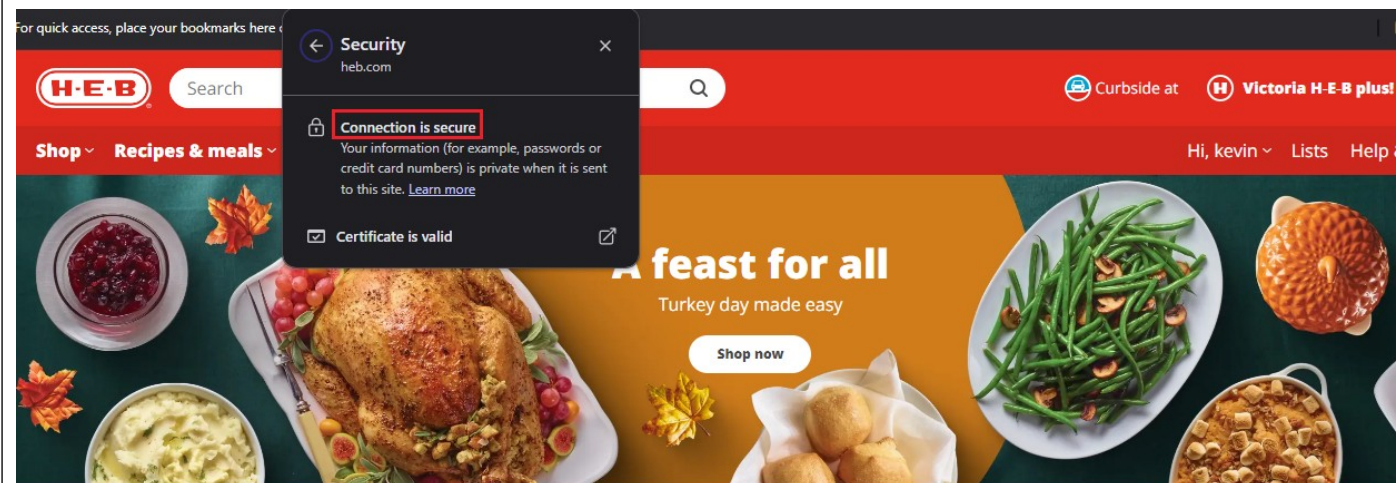
	<div data-bbox="656 194 1637 703"><p>Security overview</p><p>  </p><div data-bbox="680 300 1003 344"><p>This page is secure (valid HTTPS).</p></div><p> Certificate - valid and trusted</p><p>The connection to this site is using a valid, trusted server certificate issued by DO_NOT_TRUST_FiddlerRoot.</p><p>View certificate</p><p> Connection - secure connection settings</p><p>The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-384, and AES_256_GCM.</p><p> Resources - all served securely</p><p>All resources on this page are served securely.</p></div> <p>https://www.heb.com/</p> <div data-bbox="656 778 2033 1185"><p>Request Headers [Raw] [Header Definition]</p><p>GET /interaction/1zgnlrTkTTCH_CdY61S7VQ?prompt=register HTTP/1.1</p><p>Referer: https://www.heb.com/</p><p>Security</p><p>sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"</p><p>sec-ch-ua-mobile: ?0</p><p>sec-ch-ua-platform: "Windows"</p><p>Sec-Fetch-Dest: document</p><p>Sec-Fetch-Mode: navigate</p><p>Sec-Fetch-Site: same-site</p><p>Sec-Fetch-User: ?1</p><p>Upgrade-Insecure-Requests: 1</p><p>Transport</p><p>Connection: keep-alive</p><p>Host: accounts.heb.com</p></div>
<p>using the computer system to receive a first signal from the computer</p>	<p>Source: Fiddler capture of the accused instrumentality</p> <p>The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a first signal (e.g., a session set response, etc.) from the computer (e.g., server of the accused</p>

providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;

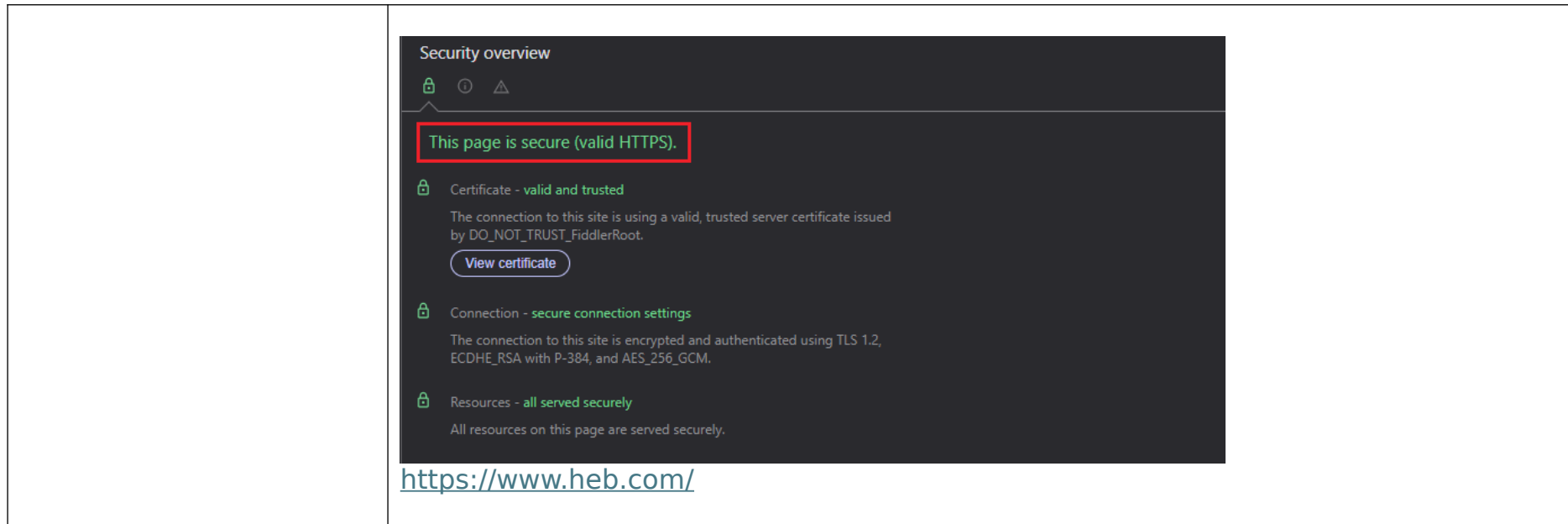
instrumentality) providing the secured capability (e.g., secure connection with the website, etc.), the first signal comprising a reusable identifier (e.g., `_SESSION`, etc.) corresponding to the secured capability (e.g., secure connection with the website, etc.), the reusable identifier assigned for use by the secured capability for a finite period of time (e.g., Expiry period).

As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, food searches, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. The server sends a response to set `_SESSION` value, which is set by the user device.

As shown, the `_SESSION` token set by the end device is reused in all further communications with the server. The `_SESSION` token also mentions an Expiry period for the token, indicating that it can be reused for a finite period.



<https://www.heb.com/>



Security

sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1

Transport

Connection: keep-alive
Host: accounts.heb.com

TransformerHeadersTextViewSyntaxViewImageViewHexViewWebViewAuthCachingCookiesRawJSONXML

Set-Cookie: _interaction_resume=9pVs4kNfnKJSwWBvIjWj2; path=/oidc/auth/9pVs4kNfnKJSwWBvIjWj2; expires=Thu, 21 Nov 2024 10:21:18 GMT; samesite=lax; secure; httponly

Response sent 161 bytes of Cookie data:
Set-Cookie: _interaction_resume.sig=0xpu0S8pdTe34_2YF5qxMzo8Zt4; path=/oidc/auth/9pVs4kNfnKJSwWBvIjWj2; expires=Thu, 21 Nov 2024 10:21:18 GMT; samesite=lax; secure; httponly

Response sent 110 bytes of Cookie data:
Set-Cookie: _session=8RAkBEHgdxm8VxaXWdtm_; path=/; samesite=none; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

Response sent 120 bytes of Cookie data:
Set-Cookie: _session.sig=TPNbNBEK7w8GWFoKjm1JFL4EjVQ; path=/; samesite=none; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

Response sent 102 bytes of Cookie data:
Set-Cookie: _session.legacy=8RAkBEHgdxm8VxaXWdtm_; path=/; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

receive a first signal from a computer

finite period of time

Source: Fiddler captures of the accused instrumentality

The image contains two screenshots of Fiddler's Request Headers tab, illustrating the reuse of a session identifier. Both screenshots show a GET request with a long URL and a '3Htp0PwLufyNgI88yi/q+N5zwQIAjpvrrKLSPyD3QxKy3ci3dzWZlIT8l2hLsEUfK4fXeLafvSiHa==' header. The request body contains several parameters, including '_session=' which is highlighted with a red box and labeled 'reusable identifier'. The first screenshot shows a request to 'http://10.10.10.10:8080/interaction/1zgnlrTkTTCH_CdY61S7VQ?prompt=finalize HTTP/1.1'. The second screenshot shows a request to 'http://10.10.10.10:8080/oidc/auth/9pVs4kNfnKJSwWBvjWj2 HTTP/1.1'. Both requests include a 'Uza6UKnbKzUEf0ysAccUFGn7PmcAAAAAomysQtqOcj7Kg4D025vHuA==' header. The 'reusable identifier' is highlighted in red in both screenshots.

used by the user, the second signal comprising a copy of the reusable identifier and user verification information;

copy of the reusable identifier (e.g., _SESSION, etc.) and user verification information (e.g., DYN_USER_ID).

When the server sends a message containing an _SESSION to the user device, the client includes a copy of the _SESSION in all subsequent requests to the server, along with user verification information (e.g., DYN_USER_ID credentials). This allows the server to authenticate the client for the duration of the session and ensure secure communication between the client and server.

The screenshot displays the 'Request Headers' section of a network capture. The request is a GET to '/oidc/auth/9pVs4kNfnKJSwWBvjWj2 HTTP/1.1'. The headers include several cookies and session identifiers. One header, '_session=8RAkBEHgdxm8VxaXWdtm_', is highlighted with a red box and labeled 'reusable identifier'. Other headers include '_interaction_resume.sig=0xpu0S8pdTe34_2YF5qxMzo8Zt4', '_session.legacy.sig=UyZTnW8407JSvRWm61MnyYM1L0', and 'incap_ses_1447_2576970'.

```
GET /oidc/auth/9pVs4kNfnKJSwWBvjWj2 HTTP/1.1
3Htp0PwlufyNgl88yi/q+N5zwQIAjpvrrKLSpyD3QxFky3ci3dzWZliIT8l2hLsEUfK4fXelafvSIhA==
_interaction_resume.sig=0xpu0S8pdTe34_2YF5qxMzo8Zt4
_interaction_resume=9pVs4kNfnKJSwWBvjWj2
_session.legacy.sig=UyZTnW8407JSvRWm61MnyYM1L0
_session.legacy=8RAkBEHgdxm8VxaXWdtm_
_session.sig=TPNbNBK7w8GWFOkjm1JFL4EjVQ
_session=8RAkBEHgdxm8VxaXWdtm_ reusable identifier
_uad=eyJhbGciOiJIUzI1NiIsImtpZCI6IktkMVNfeXRheExWNGpPWXRSWUNpOFFESDQxZmJoTGI5WldRUnBYZ1dPdFkifQ.eyJleHQiOiIwbktHTk0wZjdMN2Q1MEJvb2lXNyIsI
AMP_760524e2ba=JTdCJTJyZGV2aWNISWQIMjIM0EIMjJoLTU3YzU5MjZmLTUyNGYtNDc2Yy05ZjYSLWY4YzgyZmJhNjk0NCUyMiUyYyUyMnNlc3Npb25JZCUyMiUzQTE3MzIz
AMP_MKTG_760524e2ba=JTdCJTdE
incap_ses_1447_2576970
Uza6UKnbKzUEf0ysAccUFGn7PmcAAAAAomysQtqOcj7Kg4D025vHuA==
incap_ses_32_2576970
```

Source: Fiddler Capture of the accused instrumentality

Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML
<p>Request sent 2581 bytes of Cookie data:</p> <pre>_interaction_resume=9pVs4kNfnKJSwWBvIjWj2 _interaction_resume.sig=0xpu0S8pdTe34_ZYF5qxMzo8Zt4 visid_incap_2302070=XA8WZo6vRWCLHWvz1ZY6Fyj5PmcAAAAAQUIPAAAAAAD1WM6b0WIDIPyggZK15Syb incap_ses_704_2302070= fbIkAh8OYhZrj+7EZRzFCSn5PmcAAAAAo/7RwMDCFBRCV3xHxIMWQ== AMP_MKTG_760524e2ba=JTdCJTdE _ga=GA1.1.668622678.1732180267 _gd_au=1.1.79474892.1732180268 OptanonConsent= isGpcEnabled=0 datestamp=Thu+21+2024+14%3A41%3A24+GMT%2B0530+(India+Standard+Time) version=202405.2.0 browserGpcFlag=0 isIABGlobal=false hosts= consentId=444f7245-ed51-43c0-bf88-131bfe46ca3e interactionCount=1 isAnonUser=1 landingPath=https%3A%2F%2Fwww.heb.com%2F groups=C0004%3A1 AMP_ 760524e2ba=JTdCJTdEYGV2aWNISWQIMjIIM0EIMjJoLTU3YzU5MjZmLTU2NGYtNDc2Yy05ZjY5LWY4YzgyZmJhNjk0NCUyMiUyQyUyMnNlc3Npb25JZCUyMiUzQTE3MzIxODAyNjY4MzUIMkMIMjJvdHRpdX QIMjIIM0FmYWxzZSUyQyUyMmxhc3RFdmVudFRpbWUIMjIIM0ExNzMyMTgwMjg0MDgwJTdCJTdEYGFzdEV2ZW50SWQIMjIIM0E5JTdCJTdEYGFnZUNvdW50ZXIIMjIIM0EwJTdE visid_incap_2576970=te0VLCy/Sok3BtA7WghsNj35PmcAAAAAQUIPAAAAAAAY4pR+2mtUQbfyKHJuDL7H incap_ses_32_2576970= IpMiNKlpChnbAtFECrBxAD35PmcAAAAAz2nFJAuUw4UuZFB2g5VbA== _ga_WKSH6HYPT4=GS1.1.1732180267.1.0.1732180287.0.0.0</pre>									
<p>Source: Fiddler capture of the accused instrumentality</p>									

Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML
	<pre> groups=C000170011 AMP_ 760524e2ba=JTdCJTtyZGV2aWNSISWQIMjIIM0EIMjJoLTU3YzU5MjZmLTU2NGYtNDc2Yy05ZjY5LWY4YzgyZmJhNjK0NCUyYUyQyUyMnNlc3Npb25JZCUyMiUzQTE3MzIxODAyNjY4MzUIMkMIMjJvcHRpdX QIMjIIM0FmYXZzSUyYyUyMmhc3RfMmVudFRpbWUIMjIIM0EIMjJoLTU3YzU5MjZmLTU2NGYtNDc2Yy05ZjY5LWY4YzgyZmJhNjK0NCUyYUyQyUyMnNlc3Npb25JZCUyMiUzQTE3MzIxODAyNjY4MzUIMkMIMjJvcHRpdX visid_incap_2576970=te0VLcy/Sok3BtA7WghsNj35PmcAAAAAQUIPAAAAAA4pR+2mtUQbFyKHJuDL7H incap_ses_32_2576970= IpMiNkQpChnbAtFECrBxAD35PmcAAAAA2hFJAuUw4UuZFB2g5VbA== _ga_WKSH6HYPT4=GS1.1.1732180267.1.0.1732180287.0.0.0 reese84= 3:px5OhuTal52ztIXpwGXT0Q==:vrNp79/awEwXe1SE2Ru+ 7N25rYHDIn324fNGrm4CI0USCxuRhgzr9AYoDchPhKCHzinV5125OAYwf3tWg//ZDqpFdGdfl2sR9S+rEA2GloZ0hQkNLmar2J+ 28TP8gjh1wxgv9sp3DFeKuXpZWOVbFnZ9R5SrnkHEjNbxkKlKAYrVQHfVZolRxhg19xK0+vSlrYJRTNB3hzc9A78RD8dat9CNT458DgU4gIRyCFQTodpVsamFEgF61XUTBrIMXuA4imYf+ 9PbIPC7Jluwonda4uX1x2xpQJIMU4pH3IrieolIbxrd6BDErwVTvZG2hyx2fRnQSCo1Q/Jyz9kfjNcossHs8nqAAA+L/TnmvVkk/75ReZrvXikr8Y9LkdBzxw16w5cb6T7uryl0EwbluwLcN/oJdTUGfWUa085Iny A6yNn8KZc8LAXb7qQJ0MOKJAOImTsdmUgb45IRWlwF7ht/zaLOAarUfj4ezIZOc=:9Jyx119Kq2WUfH0LWT+/aWfAVnIdrTK/vHQmbVdies= _iidt= 3Htp0PwluFyNgl88yi/q+N5zwQIAjpvvrKLSpyD3QxFky3ci3dzWZiit8l2hLseUfK4fXeLafvSIhA== incap_ses_1447_2576970= Uza6UKnbKzUEf0ysAccUFgn7PmcAAAAAomysQtQc7Kg4D025vHuA== _uad=eyJhbGciOiJIUzI1NiIsImtpZCI6Ikt0bWVneXhRheExWNGpPWXRWUWUWpOFFESDQxZm0tTGl5SWdRUnBYZD1pdFkiQ.eyJleHQiOiIwbkthTkw0wZjdMN2Q1MEJvb2lXNyIsImhhdCI6MTczMjE 4MDg3N30.qrUsVrT6yTaU7xxwEZbQYxhKptY8GS2QS9dWdu5ryOTc7liuj4H7gvebYZ7uutYuUHCXs27v- Ww0vwI3W1zmCQr8vs7dtUND4Go1yfqHcdMt7ZM0I3VHdC6LFCM2vE1qLZvmtgiqDSuBWFxncc370IUE78RM9Apz8R2Z0buHhXns3QZ_nRbmn1751-NyX2m-ivR.JnTC57MHZFp- YUTFJCYlUK1OK91BZ-zBQkrrcm14nA-zQB8oT_gmy4PO4jhLobpA0_SFqBLCbiYtP0dFOLHU40r1i4_K7RV2667ibiSuAvTR3ix9iza9NihTdRdyPkF1_F4dD-7zGdUtVh1Zg _session=8RAkBEHgdxm8VxaXWdtm _session.sig=TPNDBEK7w8GwF0KjM1JFL4EjVQ _session.legacy=8RAkBEHgdxm8VxaXWdtm _session.legacy.sig=UyZTNW8407JJSvRWm61MnyYMILO </pre>								
	<p>Source: Fiddler capture of the accused instrumentality</p> <pre> HEB_AMP_DEVICE_ID=h-57c5926f-664f-476c-9f69-f8c82fba6944 AWSALB=NZxazoCm8CI7brJY/xCGvn9RvcwLLDHcThTb3khhb9uO2rTEtxBdaUuHZGLjEOhJsATlcCU iggYSeuggBSuEhtg1UTor/0NHOUhDiB31eDIYn4PjZieYcroJDkP2 DYN_USER_ID=19145584007 DYN_USER_CONFIRM=0a8f34973579389ff6e6623cdc525b8c USER_SELECT_STORE=false CURR_SESSION_STORE=92 sessionContext=curbside JSESSIONID=XOV0op84uxVvner6PVFnXR008qCjrPESzofBcz1o sst=hs:sst:J1SQw96x6Ta1weQM4wsdY sst.sig=vUQ1uMxDrUPupjFbrxvUa5qHW5B1B4XkvIKFg67Y9so visid_incap_2302070 </pre>								

	Source: Fiddler capture of the accused instrumentality
using a processor of the computer system to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and	<p>The accused instrumentality practices using a processor of the computer system (e.g., processor of the authentication server of the accused instrumentality, etc.) to evaluate, based at least on the first signal (e.g., a _SESSION set response, etc.) and the second signal (e.g., a request signal from the user device), whether the user is authorized to conduct the at least one interaction (e.g., account login, food searches, etc.) with the secured capability (e.g., secure connection with the website, etc.).</p> <p>The server compares the reusable identifier, such as the token (e.g., _SESSION), in the first response received from the server with the token included in the client's subsequent request. If a match is found, the server authenticates the user and processes the request securely.</p>

Security

sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1

Transport

Connection: keep-alive
Host: accounts.heb.com

TransformerHeadersTextViewSyntaxViewImageViewHexViewWebViewAuthCachingCookiesRawJSONXML

Set-Cookie: _interaction_resume=9pVs4kNfnKJSwWBvIjWj2; path=/oidc/auth/9pVs4kNfnKJSwWBvIjWj2; expires=Thu, 21 Nov 2024 10:21:18 GMT; samesite=lax; secure; httponly

Response sent 161 bytes of Cookie data:
Set-Cookie: _interaction_resume.sig=0xpu0S8pdTe34_2YF5qxMzo8Zt4; path=/oidc/auth/9pVs4kNfnKJSwWBvIjWj2; expires=Thu, 21 Nov 2024 10:21:18 GMT; samesite=lax; secure; httponly

Response sent 110 bytes of Cookie data:
Set-Cookie: _session=8RAkBEHgdxm8VxaXWdtm_; path=/; samesite=none; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

Response sent 120 bytes of Cookie data:
Set-Cookie: _session.sig=TPNbNBEK7w8GWFokJm1JFL4EjVQ; path=/; samesite=none; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

Response sent 102 bytes of Cookie data:
Set-Cookie: _session.legacy=8RAkBEHgdxm8VxaXWdtm_; path=/; secure; httponly; expires=Sat, 21 Dec 2024 09:21:18 GMT

receive a first signal from a computer

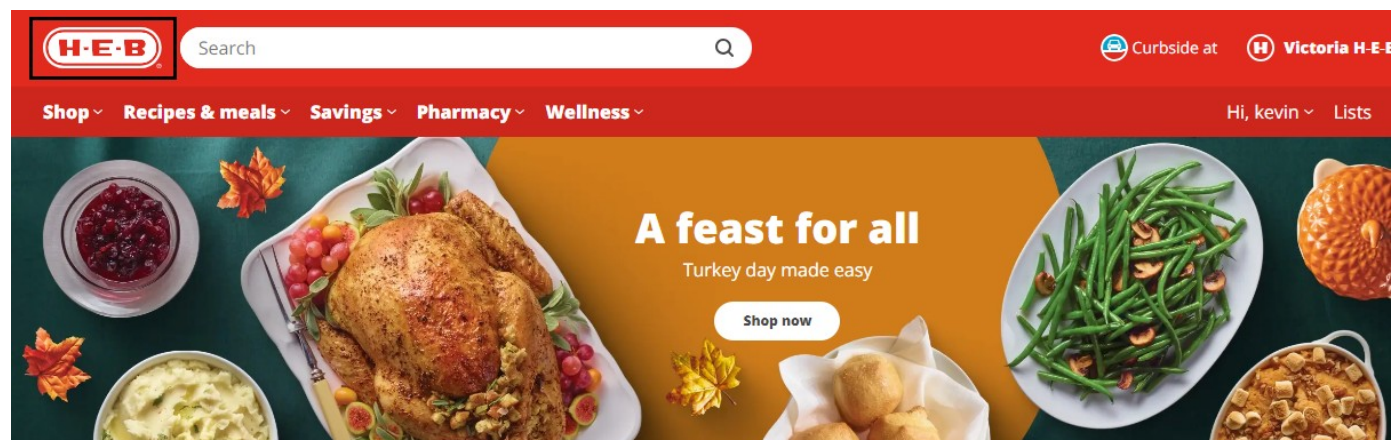
finite period of time

Source: Fiddler captures of the accused instrumentality

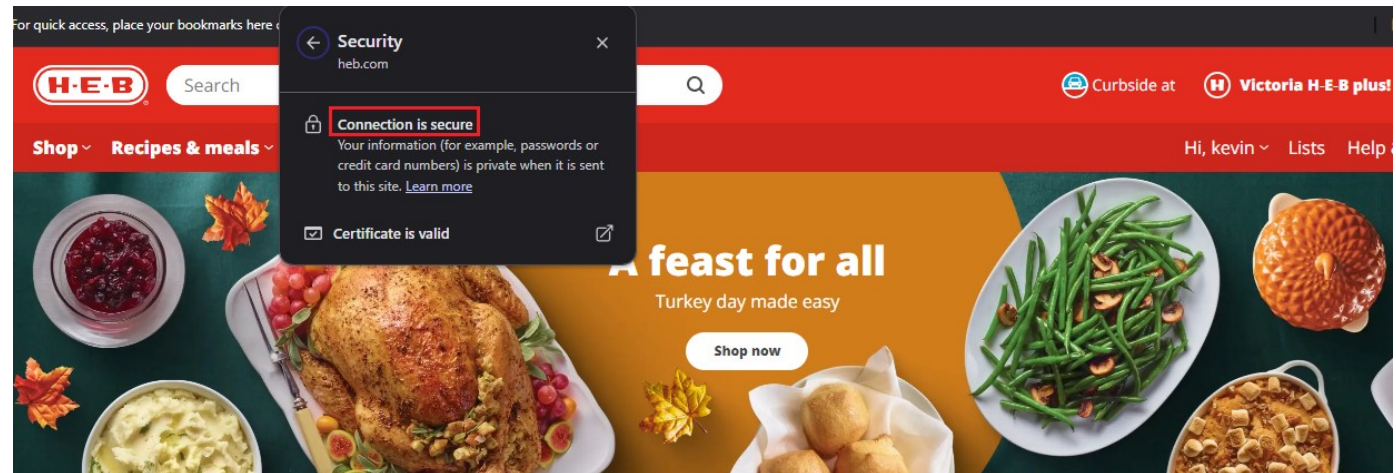
Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML
<pre> groups=C000170011 AMP_ 760524e2ba=JTdCJTtyZGV2aWNSISWQIMjIM0EIMjJoLTU3YzU5MjZmLTU2NGYtNDc2Yy05ZjY5SLWY4YzgyZmJhNjK0NCUyMiUyQyUyMnNlc3Npb25JZCUyMiUzQTE3MzIxODAyNjY4MzUIMkMIMjJvcHRPdX QIMjIM0FmYWxzZSUyQyUyMmMxc3RFRmVudFRpbWUIMjIM0EIMjJoLTU3YzU5MjZmLTU2NGYtNDc2Yy05ZjY5SLWY4YzgyZmJhNjK0NCUyMiUzQTE3MzIxODAyNjY4MzUIMkMIMjJvcHRPdX visid_incap_2576970=te0VLcy/Sok3BtA7WghsNj35PmcAAAAAQUIPAAAAAA4pR+2mtUQbfyKHJuDL7H incap_ses_32_2576970= IpMiNkPChnbAtFEcRbXAD35PmcAAAAA2hFJAuUw4UuZFB2g5VbA== _ga_WKSH6HYPT4=GS1.1.1732180267.1.0.1732180287.0.0.0 reese84= 3:px5Ohtal52ztIXpwGXT0Q==:vrNp79/awEwXe1SE2Ru+ 7N25rYHDIn324fNGm4C10USCxuRhgzr9AYoDcHphKCHzinV5125Oaywf3tWg//ZDqpFdGdfl.2sR9S+reA2G1oZ0hQkNLmar2J+ 28TP8gjh1wxgv9sp3DFeKuXpZWOVbFnZ9R5SrnkHEjNbxKlKAYrVQHfVZolRxhg19xk0+vsLrYJRTNB3hzc9A78RD8dat9CNT458DgU4gIRyCFQITodpVsamFEgF61XUTBrIMXuA4imYf+ 9PbIPC7Jluwonda4uX1x2xpQJIMU4pH3IrieolIbXrd6BDErWVTvZG2hyx2fRNQSCo1Q/Jyz9kfNcossHs8nqAAA+L/TnmvVkk/75RezrvXikr8Y9LkdBzxw16w5cb6T7uryl0EwbluwLcN/oJdTUGfWUa085Iny A6yNn8kZc8LAXb7qQJ0MOKJAOImTsdmUgb45IRWlwF7ht/zaLOAarUfj4ezIZOc=:9Jyx119Kq2WUfH0LWT+/aWfAvnidrTK/vHQmbVdies= _iidt= 3Htp0PwluFyNgl88yi/q+N5zwQIAjpvvrKLSpyD3QxFky3ci3dzWZlilt8l2hLseUfK4fXeLafvSIhA== incap_ses_1447_2576970= Uza6UKnbKzUEf0ysAccUFGn7PmcAAAAAomysQtQcJ7Kg4D025vHuA== _uad=eyJhbGciOiJIUzI1NiIsImtpZCI6IkhkMVNfeXRheExWNGpPWXR5WUNPFFESDQxZmJoTG15WldRUnBYZD1PdFkiQy.eyJleHQiOiIwbkthTkwZjdMNQ2IMEjvb2lXNyIsImhhdCI6MTczMjE 4MDg3N30.qrUsvrT6yTaU7xxwEZbQYxhKpTy8GS2QS9dWdu5ryOTc7iuj4H7gvebY2ZtuUyUHCpXs27v- Ww0vwI3W1zmCQr8vs7dtUND4Go1yfqHcdMt7ZM0I3VHdC6LFCM2vE1qLZvmtgiqDSuBWFxncc370IUE78RM9Apz8R2Z0buHhXns3QZ_nRbmn1751-NyX2m-IVR.JnTC57MHZFp- YUTFJCYlUK1OK91B7-zBQkrrcm14nAzQB8oT_gmy4PO4jhLobpA0_SFoBlChiyP0dFOLHU40r1i4_K7Rv2667ibiSuAvTR3ix9iza9NihTdrdyPkF1_F4dD-7zGdUtVh1Zg _session=8RAkBEHgdxm8VxaXWdtm _session.sig=TPNDVBK7W8GWF0KjM1JFL4EjVQ _session.legacy=8RAkBEHgdxm8VxaXWdtm _session.legacy.sig=UyZTnW8407JJSvRWm61MnyYMILO </pre>									

the second signal comprising the copy of the reusable identifier

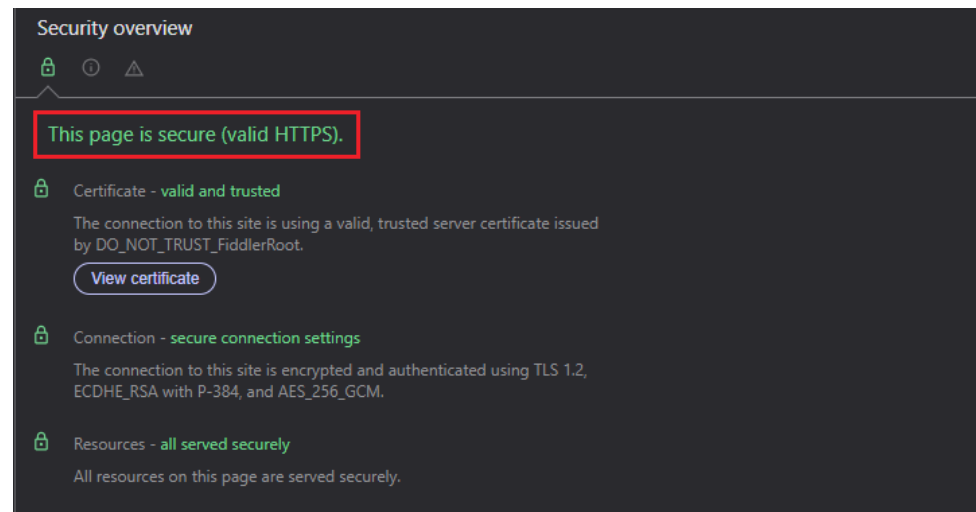
Source: Fiddler capture of the accused instrumentality



<https://www.heb.com/>



<https://www.heb.com/>

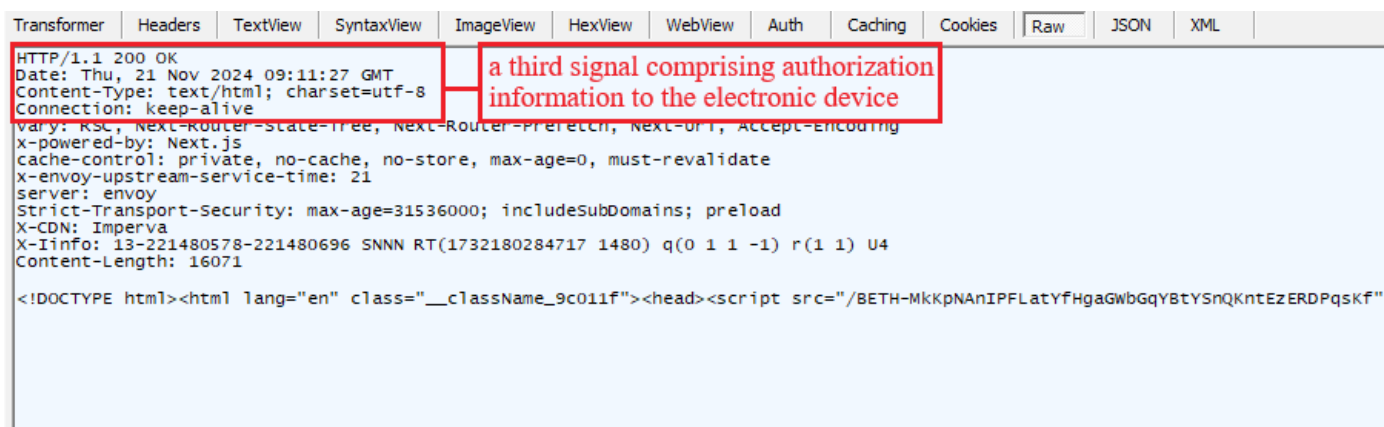


<https://www.heb.com/>

in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal comprising authorization information to at least one of the electronic device and the computer.

The accused instrumentality practices in response to an indication from the processor (e.g., processor of the authentication server of the accused instrumentality, etc.) that the user is authorized to conduct the at least one interaction with the secured capability (e.g., secure connection with the website, etc.), using the computer system processor (e.g., authentication server of the accused instrumentality, etc.) to transmit a third signal comprising authorization information (e.g., a response signal from the server to the user device, etc.) to at least one of the electronic device (e.g., user device, etc.) and the computer.

As shown, upon authenticating the _SESSION, the user device receives an authentication confirmation message (a third signal), from the server to the user device.



Source: Fiddler capture of the accused instrumentality

